ADOA/ISD/ISS
Monthly Cyber Security Tips
NEWSLETTER

AUGUST 2006 Volume 1, Issue 3

Erasing Information and Disposal of Media

From the Desk of Information Security Services

Protecting confidential and sensitive data from accidental disclosure is very important, and we should all strive to properly handle data erasure and the disposal of media.

How can I be sure files are erased?

Data can be stored electronically in multiple formats and locations. Data sometimes includes sensitive documents or possibly data containing personally identifiable information such as a social security number, credit card information, or health related information. For example, the initial information may arrive on a CD and then copied to the computer's hard drive and subsequently backed up for disaster recovery purposes. In this example, there are three different storage mediums: CD, Hard Drive and backup media. In addition, just viewing a file stored on a CD can create a temporary image of the information on the computer's hard drive as well.

Deleting files does not erase the information. It only makes the space containing the files available to store additional data. The information can often be retrieved by using forensics or other recovery tools. As new computers are purchased, older computers may be sold or surplused. You should assume that sensitive information may have been stored or viewed on all computers at some point in time. Before discarding your computer or portable storage devices, you need to be sure that that data has been erased or "wiped".

What type of "wiping" program should be used?

Read/writable media (including your hard drive) should be "wiped" using Department of Defense (DOD) compliant software. Software that meets DOD compliance standards can be downloaded from the Internet at no cost.

You need to be aware of some issues in wiping data including:

- The wiping software needs to be used correctly with all the appropriate options and switches set properly.
- It may take a long time to rewrite the drive or media.
- You can't wipe a defective drive.

What about "Write Once" media, such as some CDs and DVDs?

Certain media can be read many times but can only be written once. This type of media, usually CD's or DVD's, cannot be overwritten to ensure the erasure of sensitive information. Therefore, this type of media should be physically destroyed. Certain types of shredders are capable of shredding CD's and DVD's. If this type of shredder is not available then safely breaking the device into four or more pieces would be an appropriate destruction measure.

I've heard of "degaussing", but what is it?

Degaussing is the erasure of information through the use of a very strong magnet generally used for erasing of magnetic tape media. This type of storage media is utilized by organizations with large data processing operations.

Can I just physically destroy the storage media?

Yes. Media that does not have a need to be re-used can be and probably should be physically destroyed. Media that contains sensitive or private data that cannot be "wiped" should be physically destroyed.

What about a defective drive that is under warranty?

Most warranties require the buyer to return the defective drive in order for a replacement to be provided under a warranty program. Check to be sure that your vendor has a policy that these "defective" drives are physically destroyed. There have been reports that these drives are sometimes fixed and resold without the removal the data. Be careful in these situations. Balance the risk of information being compromised versus the cost of the hard drive.

Do these procedures apply to businesses as well as home users?

Yes. However, businesses should maintain a log of all devices that have been disposed. The log should include the date, type of device, manufacturer, serial number (if one exists), destruction method used, and disposal method such as sold, crushed, or shredded.

Brought to you by:

MS-ISAC

http://www.msisac.org